I CLAIM:

1. A method for protecting decrypted digital data, to which encrypted digital data is decrypted, from illegitimate use, said method comprising the steps of:

encrypting said decrypted digital data by using a changeable key to digital data re-encrypted by the changeable key;

encrypting said digital data re-encrypted by the changeable key by using an unchangeable key in a device to digital data double re-encrypted by changeable-unchangeable keys to be stored, copied or transferred;

decrypting said copied, stored or transferred digital data double re-encrypted by changeable-unchangeable keys, by using said unchangeable key to digital data re-encrypted by the changeable key; and

decrypting said digital data re-encrypted by the changeable key, by using said changeable key to said decrypted digital data.

2. A method for protecting decrypted digital data, to which encrypted digital data is decrypted, from illegitimate use, comprising the steps of:

encrypting said decrypted digital data by using an unchangeable key in a device to digital data re-encrypted by the unchangeable key;

encrypting said digital data re-encrypted by the unchangeable key by using a changeable key to digital data double re-encrypted by changeable-unchangeable keys to be stored, copied or transferred;

decrypting said copied, stored or transferred digital data double re-encrypted by changeable-unchangeable keys, by using said changeable key to digital data re-encrypted by the changeable key; and

decrypting said digital data decrypted by the changeable key key, by using said unchangeable key to said decrypted digital data.

3. The method according to claim 1 or 2, wherein said steps of encrypting and decrypting by using said changeable key are carried out by a software.

4. The method according to claim 1 or 2, wherein said steps of encrypting and decrypting by using said changeable key are carried out by a hardware.

5. The method according to claim 1 or 2, wherein said changeable key is supplied from the outside of a device.

6. The method according to claim 1 or 2, wherein said changeable key is generated in a device.

7. The method according to claim 1 or 2, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a software.

8. The method according to claim 1 or 2, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a hardware.

9. The method according to claim 1 or 2, wherein said unchangeable key is already placed in said device.

10. The method according to claim 1 or 2, wherein said unchangeable key is generated in said device.

11. The method according to claim 1 or 2, wherein said unchangeable key is supplied from the outside of said device.

12. The method according to claim 9, 10 or 11, wherein said unchangeable key is specific to said device.

13. The method according to claim 9, 10 or 11, wherein said unchangeable key is not specific to said device.

14. An apparatus for protecting decrypted digital data, to which encrypted digital data is decrypted, from illegitimate use, said apparatus comprising:

a changeable key re-encryption unit for encrypting said decrypted digital data by using a changeable key to digital data re-encrypted;

an unchangeable key encryption unit for encrypting said digital data re-encrypted by the changeable key by using an unchangeable key in a device to digital data double re-encrypted by changeable-unchangeable keys to be stored, copied or transferred;

an unchangeable key decryption unit for decrypting said copied, stored or transferred digital data double re-encrypted by changeable-unchangeable keys, by using said unchangeable key to digital data re-encrypted by the unchangeable key; and

a changeable key decryption unit for decrypting said digital data re-encrypted by the unchangeable key, by using said changeable key to said decrypted digital data.

15. An apparatus for protecting decrypted digital data, to which encrypted digital data is decrypted, from illegitimate use, said apparatus comprising:

an unchangeable key encryption unit for encrypting said decrypted digital data by using an unchangeable key in a device to digital data re-encrypted by the unchangeable key;

a changeable key encryption unit for encrypting said digital data re-encrypted by the unchangeable key by using a changeable key to digital data double re-encrypted by changeable-unchangeable keys to be stored, copied or transferred;

a changeable key decryption unit for decrypting said copied, stored or transferred digital data double re-encrypted by changeable-unchangeable keys, by using said changeable key to digital data re-encrypted by the unchangeable key; and

an unchangeable key decryption unit for decrypting said digital data re-encrypted by the unchangeable key, by using said unchangeable key to said decrypted digital data.

16. The apparatus according to claim 14 or 15, in which encrypting and decrypting by using said changeable key are carried out by a software.

17. The apparatus according to claim 14 or 15, in which encrypting and decrypting by using said changeable key are carried out by a hardware.

18. The apparatus according to claim 14 or 15, wherein said changeable key is supplied from the outside of a device.

19. The apparatus according to claim 14 or 15, wherein said changeable key is generated in a device.

20. The apparatus according to claim 14 or 15, in which encrypting and decrypting by using said unchangeable key are carried out by a software.

21. The apparatus according to claim 14 or 15, in which encrypting and decrypting by using said unchangeable key are carried out by a hardware.

22. The apparatus according to claim 14 or 15, wherein said unchangeable key is already placed in said device.

23. The apparatus according to claim 14 or 15, wherein said unchangeable key is generated in said device.

24. The apparatus according to claim 14 or 15, wherein said unchangeable key is supplied from the outside of said device.

25. The apparatus according to claim 14 or 15, wherein said unchangeable key is specific to said device.

26. The apparatus according to claim 14 or 15, wherein said unchangeable key is not specific to said device.

27. A method for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said method comprising the steps of:

encrypting said decrypted digital data by using a second changeable key to digital data re-encrypted by the second changeable key;

encrypting said digital data re-encrypted by the second changeable key by using an unchangeable key in a device to digital data double re-encrypted by unchangeable-second-changeable keys to be stored;

decrypting said stored digital data double re-encrypted by unchangeable-second-changeable keys by using said unchangeable key to said digital data re-encrypted by the second changeable key;

encrypting said digital data re-encrypted by the second changeable key by using a third changeable key to digital data double re-encrypted by third-changeable-second-changeable keys to be copied or transferred;

decrypting said copied or transferred digital data double re-encrypted by third-changeable-second-changeable keys by using said third changeable key to digital data re-encrypted by the second changeable key; and

decrypting said digital data re-encrypted by the second changeable key by using said second changeable key to decrypted digital data.

28. A method for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said method comprising the steps of:

encrypting said decrypted digital data by using a second changeable key to digital data re-encrypted by the second changeable key;

encrypting said digital data re-encrypted by the second changeable key by using an unchangeable key in a device to digital data double re-encrypted by unchangeable-second-changeable keys to be stored;

decrypting said stored digital data double re-encrypted by unchangeable-second-changeable keys by using said unchangeable key to said digital data re-encrypted by the second changeable key;

encrypting said digital data re-encrypted by the second changeable key by using a third changeable key to digital data double re-encrypted by third-changeable-second-changeable keys to be copied or transferred;

decrypting said copied or transferred digital data double re-encrypted by third-changeable-second-changeable keys by using said third changeable key to digital data re-encrypted by the second changeable key; and

decrypting said digital data re-encrypted by the second changeable key by using said second changeable key to decrypted digital data.

29. A method for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said method comprising the steps of:

encrypting said decrypted digital data by using an unchangeable key in a device to digital data re-encrypted by the unchangeable key, and encrypting said digital data re-encrypted by the unchangeable key by using a second changeable key to digital data double re-encrypted by second-changeable-unchangeable keys to be stored;

decrypting said stored digital data double re-encrypted by second-changeable-unchangeable keys by using said second changeable key to digital data re-encrypted by the unchangeable key;

decrypting said digital data re-encrypted by the unchangeable key by using said unchangeable key to decrypted digital data;

encrypting said decrypted digital data by using a third changeable key to digital data re-encrypted by the third changeable key, and encrypting said digital data re-encrypted by the third changeable key to digital data double re-encrypted by second-changeable-third-changeable keys to be copied or transferred;

decrypting said copied or transferred digital data double re-encrypted by second-changeable-third-changeable keys by using said second changeable key to digital data re-encrypted by the third changeable key; and

decrypting said digital data re-encrypted by the third changeable key by using said third changeable key to decrypted digital data.

30. A method for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said method comprising the steps of:

encrypting said decrypted digital data by using an unchangeable key in a device to digital data re-encrypted by the unchangeable key, and encrypting said digital data re-encrypted by the unchangeable key by using a second changeable key to digital data double re-encrypted by second-changeable-unchangeable keys to be stored;

decrypting said stored digital data double re-encrypted by second-changeable-unchangeable keys by using said second changeable key to digital data re-encrypted by the unchangeable key;

decrypting said digital data re-encrypted by the unchangeable key by using said unchangeable key to decrypted digital data;

encrypting said decrypted digital data by using a third changeable key to digital data re-encrypted by the third changeable key, and encrypting said digital data re-encrypted by the third changeable key to digital data double re-encrypted by second-changeable-third-changeable keys to be copied or transferred;

decrypting said copied or transferred digital data double re-encrypted by second-changeable-third-changeable keys by using said second changeable key to digital data re-encrypted by the third changeable key; and

decrypting said digital data re-encrypted by the third changeable key by using said third changeable key to decrypted digital data.

31. The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting by using said second changeable key are carried out by a software.

32. The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting by using said second changeable key are carried out by a hardware.

33. The method according to claim 27, 28, 29 or 30, wherein said second changeable key is supplied from the outside of a device.

34. The method according to claim 27, 28, 29 or 30, wherein said second changeable key is generated in a device.

35. The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting by using said third changeable key are carried out by a software.

36. The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting by using said third changeable key are carried out by a hardware.

37. The method according to claim 27, 28, 29 or 30, wherein said third changeable key is supplied from the outside of a device.

38. The method according to claim 27, 28, 29 or 30, wherein said third changeable key is generated in a device.

39. The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a software.

40. The method according to claim 27, 28, 29 or 30, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a hardware.

41. The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is already placed in said device.

42. The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is generated in said device.

43. The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is supplied from the outside of said device.

Sub A37

44. The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is specific to a device.

45. The method according to claim 27, 28, 29 or 30, wherein said unchangeable key is not specific to a device.

46. An apparatus for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said apparatus comprising:

a second changeable key encryption unit for encrypting said decrypted digital data by using a second changeable key to digital data re-encrypted by the second changeable key;

an unchangeable key encryption unit for encrypting said digital data re-encrypted by the second changeable key by using an unchangeable key in a device to digital data double re-encrypted by unchangeable-second-changeable keys to be stored;

an unchangeable key decryption unit for decrypting said stored digital data double re-encrypted by unchangeable-second-changeable keys by using said unchangeable key to said digital data re-encrypted by the second changeable key;

a third changeable key encryption unit for encrypting said digital data re-encrypted by the second changeable key by using a third changeable key to digital data double re-encrypted by third-changeable-second-changeable keys to be copied or transferred;

a third changeable key decryption unit for decrypting said copied or transferred digital data double re-encrypted by third-changeable-second-changeable keys by using said third changeable key to digital data re-encrypted by the second changeable key; and

a second changeable key decryption unit for decrypting said digital data re-encrypted by the second changeable key by using said second changeable key to decrypted digital data.

47. An apparatus for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said apparatus comprising:

a second changeable key encryption unit for encrypting said decrypted digital data by using a second changeable key to digital data re-encrypted by the second changeable key;

an unchangeable key encryption unit for encrypting said digital data re-encrypted by the second changeable key by using an unchangeable key in a device to digital data double re-encrypted by unchangeable-second-changeable keys to be stored;

an unchangeable key decryption unit for decrypting said stored digital data double re-encrypted by unchangeable-second-changeable keys by using said unchangeable key to said digital data re-encrypted by the second changeable key;

a third changeable key encryption unit for encrypting said digital data re-encrypted by the second changeable key by using a third changeable key to digital data double re-encrypted by third-changeable-second-changeable keys to be copied or transferred;

a third changeable key decryption unit for decrypting said copied or transferred digital data double re-encrypted by third-changeable-second-changeable keys by using said third changeable key to digital data re-encrypted by the second changeable key; and

a second changeable key decryption unit for decrypting said digital data re-encrypted by the second changeable key by using said second changeable key to decrypted digital data.

48. An apparatus for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said apparatus comprising:

an unchangeable key encryption unit for encrypting said decrypted digital data by using an unchangeable key in a device to digital data re-encrypted by the unchangeable key, and a second changeable key encryption unit for encrypting said digital data re-encrypted by the unchangeable key by using a second changeable key to digital data double re-encrypted by second-changeable-unchangeable keys to be stored;

a second changeable key decryption unit for decrypting said stored digital data double re-encrypted by second-changeable-unchangeable keys by using said second changeable key to digital data re-encrypted by the unchangeable key, and an unchangeable key decryption unit for decrypting said digital data re-encrypted by the unchangeable key by using said unchangeable key to decrypted digital data;

a third changeable key encryption unit for encrypting said decrypted digital data by using a third changeable key to digital data re-encrypted by the third changeable key, and a second changeable key encryption unit for encrypting said digital data re-encrypted by the third changeable key to digital data double re-encrypted by second-changeable-third-changeable keys to be copied or transferred; and

a second changeable key decryption unit for decrypting said copied or transferred digital data double re-encrypted by second-changeable-third-changeable keys by using said second changeable key to digital data re-encrypted by the third changeable key, and a third changeable key decryption unit for decrypting said digital data re-encrypted by the third changeable key by using said third changeable key to decrypted digital data.

49. An apparatus for protecting decrypted digital data, to which digital data encrypted by a first changeable key is decrypted, from illegitimate use, said apparatus comprising:

an unchangeable key encryption unit for encrypting said decrypted digital data by using an unchangeable key in a device to digital data re-encrypted by the unchangeable key, and a second changeable key encryption unit for encrypting said digital data re-encrypted by the unchangeable key by using a second changeable key to digital data double re-encrypted by second-changeable-unchangeable keys to be stored;

a second changeable key decryption unit for decrypting said stored digital data double re-encrypted by second-changeable-unchangeable keys by using said second changeable key to digital data re-encrypted by the unchangeable key, and an unchangeable key decryption unit for decrypting said digital data re-encrypted by the unchangeable key by using said unchangeable key to decrypted digital data;

a third changeable key encryption unit for encrypting said decrypted digital data by using a third changeable key to digital data re-encrypted by the third changeable key, and a second changeable key encryption unit for encrypting said digital data re-encrypted by the third changeable key to digital data double re-encrypted by second-changeable-third-changeable keys to be copied or transferred; and

a second changeable key decryption unit for decrypting said copied or transferred digital data double re-encrypted by second-changeable-third-changeable keys by using said second changeable key to digital data re-encrypted by the third changeable key, and a third changeable key decryption unit for decrypting said digital data re-encrypted by the third changeable key by using said third changeable key to decrypted digital data.

50. The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting by using said second changeable key are carried out by a software.

51. The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting by using said second changeable key are carried out by a hardware.

52. The apparatus according to claim 46, 47, 48 or 49, wherein said second changeable key is supplied from the outside of a device.

53. The apparatus according to claim 46, 47, 48 or 49, wherein said second changeable key is generated in a device.

54. The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting by using said third changeable key are carried out by a software.

55. The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting by using said third changeable key are carried out by a hardware.

56. The apparatus according to claim 46, 47, 48 or 49, wherein said third changeable key is supplied from the outside of a device.

57. The apparatus according to claim 46, 47, 48 or 49, wherein said third changeable key is generated in a device.

58. The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a software.

59. The apparatus according to claim 46, 47, 48 or 49, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a hardware.

60. The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is already placed in the device.

61. The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is generated in the device.

62. The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is supplied from the outside of the device.

63. The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is specific to said device.

64. The apparatus according to claim 46, 47, 48 or 49, wherein said unchangeable key is not specific to said device.

65. A method for protecting digital data from illegitimate use, said method comprising the steps of:

determining whether said digital data is subject to be protected or not;

encrypting said digital data determined being subject to be protected by using an unchangeable key in said device to digital data encrypted by the unchangeable key;

storing, copying or transferring said digital data determined being not subject to be protected and said digital data encrypted by the unchangeable key;

decrypting said stored, copied or transferred digital data encrypted by the unchangeable key by using said unchangeable key to decrypted digital data; and

utilizing said stored, copied or transferred digital data and said decrypted digital data.

66. The method according to claim 65, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a software.

67. The method according to claim 65, wherein said steps of encrypting and decrypting by using said unchangeable key are carried out by a hardware.

68. The method according to claim 65, in which encrypting and decrypting by using said unchangeable key are controlled by identifying information which is added to said digital data.

69. The method according to claim 68, in which encrypting and decrypting are carried out by presence of said identifying information.

70. The method according to claim 68, in which encrypting and decrypting are carried out by absence of said identifying information.

71. The method according to claim 65, wherein said unchangeable key is already placed in a device.

72. The method according to claim 65, wherein said unchangeable key is generated in the device.

73. The method according to claim 65, wherein said unchangeable key is supplied from the outside of the device.

74. The method according to claim 71, 72 or 73, wherein said unchangeable key is specific to the device.

75. The method according to claim 71, 72 or 73, wherein said unchangeable key is not specific to the device.

76. An apparatus for protecting digital data from illegitimate use, said apparatus comprising:

determining means as to whether said digital data is subject to be protected or not;

means for encrypting said digital data determined being subject to be protected by using an unchangeable key in a device to digital data encrypted by the unchangeable key;

means for storing, copying or transferring said digital data determined being not subject to be protected and said digital data encrypted by the unchangeable key;

means for decrypting said stored, copied or transferred digital data encrypted by the unchangeable key by using said unchangeable key to decrypted digital data; and

means for utilizing said stored, copied or transferred digital data and said decrypted digital data.

77. The apparatus according to claim 76, wherein encrypting and decrypting by using said unchangeable key are carried out by a software.

78. The apparatus according to claim 76, wherein encrypting and decrypting by using said unchangeable key are carried out by a hardware.

79. The apparatus according to claim 76, wherein encrypting and decrypting by using said unchangeable key are controlled by identifying information which is added to said digital data.

80. The apparatus according to claim 76, wherein encrypting and decrypting are carried out by presence of said identifying information.

81. The apparatus according to claim 76, wherein encrypting and decrypting are carried out by absence of said identifying information.

82. The apparatus according to claim 76, wherein said unchangeable key is already placed in a device.

83. The apparatus according to claim 76, wherein said unchangeable key is generated in the device.

84. The apparatus according to claim 76, wherein said unchangeable key is supplied from the outside of the device.

85. The apparatus according to claim 82, 83 or 84, wherein said unchangeable key is specific to the device.

86. The apparatus according to claim 82, 83 or 84, wherein said unchangeable key is not specific to the device.